METHOD AND APPARATUS FOR DEFENDING AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACKS ON TCP SERVERS BY TCP STATELESS HOGS

Abstract of the Disclosure

A Distributed Denial–of-Service (DDoS) attack by a TCP stateless hog is defeated with use of an enhancement to the keep-alive mechanism provided by RFC 1122. A TCP server receives a new TCP connection request from a possible attacker and sends a keep-alive probe packet back thereto using an "invalid" sequence number. Illustratively, this "invalid" sequence number comprises a random number selected to be reasonably distant from the actual current sequence number. When a responsive packet is received from the potential attacker, the TCP server verifies the accuracy of the acknowledgement number in the received packet, thereby determining whether the potential attacker may be a TCP stateless hog.